Data Protection Policy

1. Introduction

The Production Hub Limited ("the Company" or "TPH") is committed to protecting the rights, privacy, and personal data of its staff, clients, and business contacts in line with current UK data protection laws. This includes the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR).

The Production Hub Limited is registered with the Information Commissioner's Office (ICO) as a data controller under registration number ZA089816, in compliance with the Data Protection Act 2018.

This policy outlines how we collect, use, store, share, and delete personal data, and applies to all employees, contractors, agents, and third parties acting on behalf of the Company. It should be read alongside related internal documents, including ED013 Information Security Policy, ED016 Website Privacy and TPH028 Information Security Objectives.

2. Commitment to Data Protection

TPH is committed not only to complying with data protection law, but also to fostering a culture of data responsibility and transparency. We ensure that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified, legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Retained no longer than necessary
- Protected against unauthorised access, loss, or damage

We recognise that maintaining trust is fundamental to our success as a business.

3. Scope & Responsibilities

This policy applies to all personal data processed by TPH, whether held digitally or in physical format. The Company is the Data Controller for all such data.

The Data Protection Officer (DPO) is Nick Hames (Barham Court, Teston, Maidstone, ME18 5BZ,Email: enquiries@productionhub.org.uk). The DPO is responsible for maintaining this policy, advising on compliance, and supporting responses to rights requests and breaches.

Managers are responsible for ensuring all team members understand and comply with this policy. All staff must complete data protection training at induction and follow any updates provided.

4. Lawful Basis for Processing

Personal data must be processed under a lawful basis, which may include:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data (e.g. health, ethnicity, beliefs) has additional legal requirements. The DPO should be consulted before processing such data.

TPH Collects and processes personal data collected directly from data subjects and personal data collected from third parties.

5. Data Subject Rights

Under the UK GDPR, individuals have rights including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure ("right to be forgotten")
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision-making and profiling

All requests must be handled promptly and in coordination with the DPO.

6. Consent & Marketing

Consent must be freely given, specific, informed, and unambiguous. Pre-ticked boxes or silence are not valid. Withdrawal of consent must be easy and honoured promptly.

Direct marketing requires prior consent unless the soft opt-in applies. All marketing communications must include an opt-out option.

7. Data Accuracy & Minimisation

We ensure all personal data is accurate and kept up to date. Staff must only collect and process what is necessary for their role. Excess data collection or unauthorised access is prohibited.

8. Security & Breach Response

Personal data is safeguarded through appropriate technical and organisational measures. These include:

- Role-based access controls
- Encryption
- Secure storage and backups
- Regular access reviews and system monitoring

All suspected or actual data breaches must be reported immediately to the DPO. If required, the ICO and affected data subjects will be informed within 72 hours.

9. Data Sharing & Transfers

We may share personal data with trusted service providers (e.g. print partners, IT support) under written agreements. Data will only be shared externally when legally required or necessary for service delivery.

Transfers outside the UK will only occur where adequate safeguards are in place, such as UK-approved standard contractual clauses or adequacy decisions.

10. Accountability & Governance

TPH maintains records of all data processing activities, including:

- The purposes and legal basis for processing
- Categories of data and recipients
- Retention periods
- Data security measures
- Any transfers outside the UK

We adopt a "privacy by design" approach and conduct Data Protection Impact Assessments (DPIAs) for high-risk activities. Compliance is regularly reviewed as part of our ISMS and internal audit process.

11. Definitions

For the purpose of this policy and our Data Controls the following recognised Definitions have been used

Definition	Meaning
Consent	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them
Data Controller	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to staff, customers and business contacts used in our business for our commercial purposes;
Data Processor	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
Data Subject	means a living, identified, or identifiable natural person about whom the Company holds personal data;
Personal Data	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
EEA	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
Processing	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and

Definition	Meaning
Special Category Personal Data	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

12. Key Legal References

This policy aligns with the following UK GDPR articles and Data Protection Act provisions:

- Article 5: Data Protection Principles
- Articles 6 & 9: Lawful Bases for Processing (including special category data)
- Articles 12–23: Data Subject Rights
- Article 25: Privacy by Design and DPIAs
- Articles 30 & 32: Record Keeping and Security Measures
- Articles 33 & 34: Breach Notification
- Article 44 onwards: International Transfers

This policy / policy review has been approved & authorised by:

Name and Position Nick Hames, Director/ISMS Manager

Date: 13/11/26

Signature: 

Policy Review Record	
Effective Date:	**16 March 2012**
Last Review:	**January 2026**
Next Review:	**January 2027**